

AMENDMENTS TO THE SPECIFICATION

Please delete the section entitled "SUMMARY OF THE INVENTION" in its entirety and substitute the following section therefor:

SUMMARY OF THE INVENTION

[0019] The present invention, among other applications, is directed to solving these and other problems and disadvantages of the prior art. The present invention provides a superior technique for performing cryptographic operations within a microprocessor. In one embodiment, a microprocessor apparatus is provided, for performing a cryptographic operation. The microprocessor apparatus includes an x86-compatible microprocessor that has fetch logic, a cryptography unit, and an integer unit. The fetch logic ~~disposed within a microprocessor and~~ is configured to fetch an application program from memory for execution by the x86-compatible microprocessor. The application program includes an instruction that directs the x86-compatible microprocessor to perform the cryptographic operation. The instruction has an opcode field and a repeat prefix field. The opcode field prescribes that the device accomplish the cryptographic operation as further specified within a control word stored in ~~a memory~~ the memory. The repeat prefix field is coupled to the opcode field. The repeat prefix field indicates that the cryptographic operation prescribed by the instruction is to be accomplished on a plurality of blocks of input data. The a cryptography unit is disposed within execution logic in the microprocessor, and is configured to execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, where the plurality of cryptographic rounds are prescribed by the control word. The integer unit is ~~also disposed within execution logic in the microprocessor and is~~ coupled in parallel with the cryptography unit. The integer unit is configured to execute a plurality of integer operations that are required to accomplish the cryptographic operation.

[0021] Another aspect of the present invention provides an apparatus for performing cryptographic operations. The apparatus has an x86-compatible microprocessor that includes fetch logic, translation logic, and a cryptography unit. The fetch logic fetches an

application program from memory for execution by ~~a microprocessor~~ the x86-compatible microprocessor. The application program includes a cryptographic instruction, where the cryptographic instruction prescribes one of the cryptographic operations. The cryptographic instruction includes an opcode field and a repeat prefix field. The opcode field prescribes that the circuit accomplish the cryptographic operation as further specified within a control word stored in a memory. The repeat prefix field is coupled to the opcode field. The repeat prefix field indicates that the cryptographic operation prescribed by the cryptographic instruction is to be accomplished on a plurality of blocks of input data. The translation logic ~~is disposed within the microprocessor, and~~ is configured to translate the cryptographic instruction into associated micro instructions that specify sub-operations required to accomplish the one of the cryptographic operations. The cryptography unit ~~is disposed within execution logic in the microprocessor, and~~ is configured to receive a first plurality of the associated micro instructions, and is configured to execute a plurality of cryptographic rounds on each of the plurality of blocks of input data to generate a corresponding each of a plurality of output text blocks, where the plurality of cryptographic rounds are prescribed by the control word.